



DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND

P.O. BOX 12798

FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY
REFER TO:

Battlespace Communications Portfolio (JTE)

24 Jul 07

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of Cisco 1800, 2800, 3800, and 7200 Families of Routers Running Internetwork Operating System Version 12.4(11)T for Internet Protocol Version 6 (IPv6) Capability

References: (a) DoDD 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.
2. The Cisco 1800, 2800, 3800, and 7200 Families of Routers running Internetwork Operating System (IOS) Version 12.4(11)T, hereinafter referred to as the devices under test (DUTs), meet the Internet Protocol (IP) Version 6 (IPv6) Capable interoperability requirements of the Department of Defense (DoD) Information Technology Standards Registry, "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 1," 1 June 2006, reference (c), and are certified for listing on the DoD IPv6 Approved Products List as IPv6 Capable. However, there are routers within these families (2821, 2851, 3825, 7201, 7204VXR, and 7206VXR that were not tested, but the routers are architecturally equivalent and utilize the same IOS, and JITC analysis determined them to be functionally identical for certification purposes. The Cisco 1841, 2811, 3845, and 7200 running IOS Version 12.4(11)T successfully completed the related IPv6 Performance and Interoperability portions of the DoD IPv6 Generic Test Plan (GTP) Version 3, Draft, reference (d). The DoD IPv6 GTP Version 3 includes more accurate test procedures and a complete IP Security annex and therefore was used for this test instead of the DoD IPv6 GTP Version 2. This certification expires upon changes that could affect interoperability, but no later than 3 years from the date of this memorandum.
3. This special certification is based on IPv6 Capable testing conducted by JITC at Fort Huachuca, Arizona. Testing was conducted at JITC's Advanced IP Technology Laboratory from 2 April through 8 June 2007. Enclosure 2 documents the summary test results and describes the DUTs. Users should verify interoperability before deploying the DUTs in an environment that varies significantly from that described.

JITC Memo, JTE, Special Interoperability Test Certification of Cisco 1800, 2800, 3800, and 7200 Families of Routers Running Internetwork Operating System Version 12.4(11)T for Internet Protocol Version 6 (IPv6) Capability

4. The DUTs' interoperability status summary is found in table 1 and table 2 lists the DUTs' equipment list.

Table 1. Cisco Routers Interoperability Status Summary

Cisco 1800, 2800, 3800 and 7200 Routers		
Functional Category	Critical	Verified
Base IPv6	Yes	Yes
IPSec	Yes	Yes
Transition Mechanisms	Yes	Yes
Quality of Service	Yes	Yes
Mobility	N/A	No
Network Management	Yes	Yes
Interior Router	Yes	Yes
Exterior Router	Yes	Yes
LEGEND:		
IPv6	Internet Protocol Version 6	N/A Not Applicable
IPSec	Internet Protocol Security	

Table 2. Cisco Router Equipment Listing

Cisco 1800 Router		
Component	Firmware/Software	Interface
Cisco 1841	Cisco IOS Version 12.4(11)T	RJ45 100 Mbps Ethernet
Cisco 2800 Router		
Component	Firmware/Software	Interface
Cisco 2811	Cisco IOS Version 12.4(11)T	RJ45 100 Mbps Ethernet
Cisco 3800 Router		
Component	Firmware/Software	Interface
Cisco 3845	Cisco IOS Version 12.4(11)T	RJ45 100 Mbps Ethernet
Cisco 7200 Router		
Component	Firmware/Software	Interface
Cisco 7200	Cisco IOS Version 12.4(11)T	RJ45 100 Mbps Ethernet
LEGEND:		
IOS	Internetwork Operating System	RJ Registered Jack
Mbps	Megabits Per Second	T New Technology

5. No detailed test report was written in accordance with the DoD IPv6 Master Test Plan. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet),

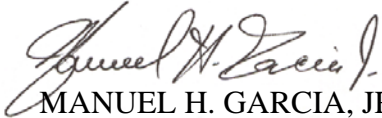
JITC Memo, JTE, Special Interoperability Test Certification of Cisco 1800, 2800, 3800, and 7200 Families of Routers Running Internetwork Operating System Version 12.4(11)T for Internet Protocol Version 6 (IPv6) Capability

or <http://199.208.204.125> (SIPRNet). Information related to IPv6 Capable testing is on the DoD IPv6 Approved Products List at http://jitc.fhu.disa.mil/adv_ip/register/register.html.

6. The JITC point of contact is Captain Richard J. Duncan, DSN 821-0154, commercial (520) 533-0154, or e-mail richard.j.duncan@disa.mil.

FOR THE COMMANDER:

2 Enclosures a/s



MANUEL H. GARCIA, JR.

Acting Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Special Interoperability Test Certification of Cisco 1800, 2800, 3800, and 7200 Families of Routers Running Internetwork Operating System Version 12.4(11)T for Internet Protocol Version 6 (IPv6) Capability

Distribution:

Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000
Office of Assistant Secretary of Defense (NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite 7000, 1851 S. Bell St., Arlington, VA 22202
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch, ATTN: GE333, Room 244, P.O. Box 4502, Falls Church, VA 22204-4502
Defense Information Systems Agency, Standards and Engineering Branch, ATTN: GE331, Bldg 283, Fort Monmouth, NJ 07703
Air Force Communications Agency/ECSS, ATTN: IPv6 Transition Office, 203 Losey St., Scott Air Force Base, IL 62225
Navy IPv6 Transition Project Office, ATTN: SPAWAR 053 OT1, 4301 Pacific Highway, San Diego, CA 92110-3127
U.S. Army, ATTN: CIO-G-6, SAIS-AOT, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Marine Corps (C4ISR), MARCORSSYSCOM, 2200 Lester St., Quantico, VA 22134-5010
DOT&E, Net-Centric Systems and Naval Warfare, 1700 Defense Pentagon, Washington, DC 20301-1700
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Chief of Naval Operations (N71CC2), CNO N6/N7, 2000 Navy Pentagon, Washington, DC 20350
Headquarters U.S. Air Force, AF/XICF, 1800 Pentagon, Washington, DC 20330-1800
Department of the Army, Office of the Secretary of the Army, CIO/G6, ATTN: SAIS-IOQ, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Coast Guard, CG-64, 2100 2nd St. SW, Washington, DC 20593
Defense Intelligence Agency, 2000 MacDill Blvd., Bldg 6000, Bolling AFB, Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD 20755-6496
Director, Defense Information Systems Agency, ATTN: GS235, Room 5W24-8A, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Under Secretary of Defense, AT&L, Room 3E144, 3070 Defense Pentagon, Washington, DC 20301
U.S. Joint Forces Command, J68, Net-Centric Integration, Communications, and Capabilities Division, 1562 Mitscher Ave., Norfolk, VA 23551-2488

ADDITIONAL REFERENCES

- (c) Department of Defense (DoD) Information Technology Standards Registry (DISR), "DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products Version 1," 1 June 2006
- (d) Joint Interoperability Test Command, "DoD IPv6 Generic Test Plan Version 3, Draft
- (e) DoD Chief Information Officer (CIO) Memorandum, "IPv6," 9 June 2003
- (f) DoD CIO Memorandum, "IPv6 Interim Transition Guidance," 29 September 2003
- (g) DoD IPv6 Transition Office, "DoD IPv6 Master Test Plan, Version 2," September 2006
- (h) DoD, "Defense Information Systems Network (DISN) Global Information Grid (GIG) Convergence Master Plan (GCMP), Version 5.25," 29 March 2006

INTERNET PROTOCOL VERSION 6 CAPABLE TESTING SUMMARY

- 1. SYSTEM TITLE.** Cisco 1800, 2800, 3800, and 7200 Family of Routers.
- 2. PROPONENT.** Department of Defense (DoD) Internet Protocol (IP) Version 6 (IPv6) Transition Office (DITO).
- 3. PROGRAM MANAGER/USER POC.** DITO, Defense Information Systems Agency, Attn: GE36 Mark Dugroo, P.O. Box 4502, Arlington, VA 22204-4502, (703) 882-0241, e-mail: mark.dugroo@disa.mil.
- 4. TESTER.** Captain Richard J. Duncan, Joint Interoperability Test Command (JITC), P.O. Box 12798, Fort Huachuca, AZ 85670-2798, DSN: 821-0154, commercial: (520) 533-0154, e-mail: richard.j.duncan@disa.mil.
- 5. DEVICE UNDER TEST DESCRIPTION.** The devices under test (DUTs) were Cisco 1841, 2811, 3845, and 7200 routers providing IPv6 capability, IP Security (IPSec) and authentication.
- 6. OPERATIONAL ARCHITECTURE.** The operational architecture was the simulated Defense Information Systems Network (DISN) IP Core Node as depicted in figure 2-1.

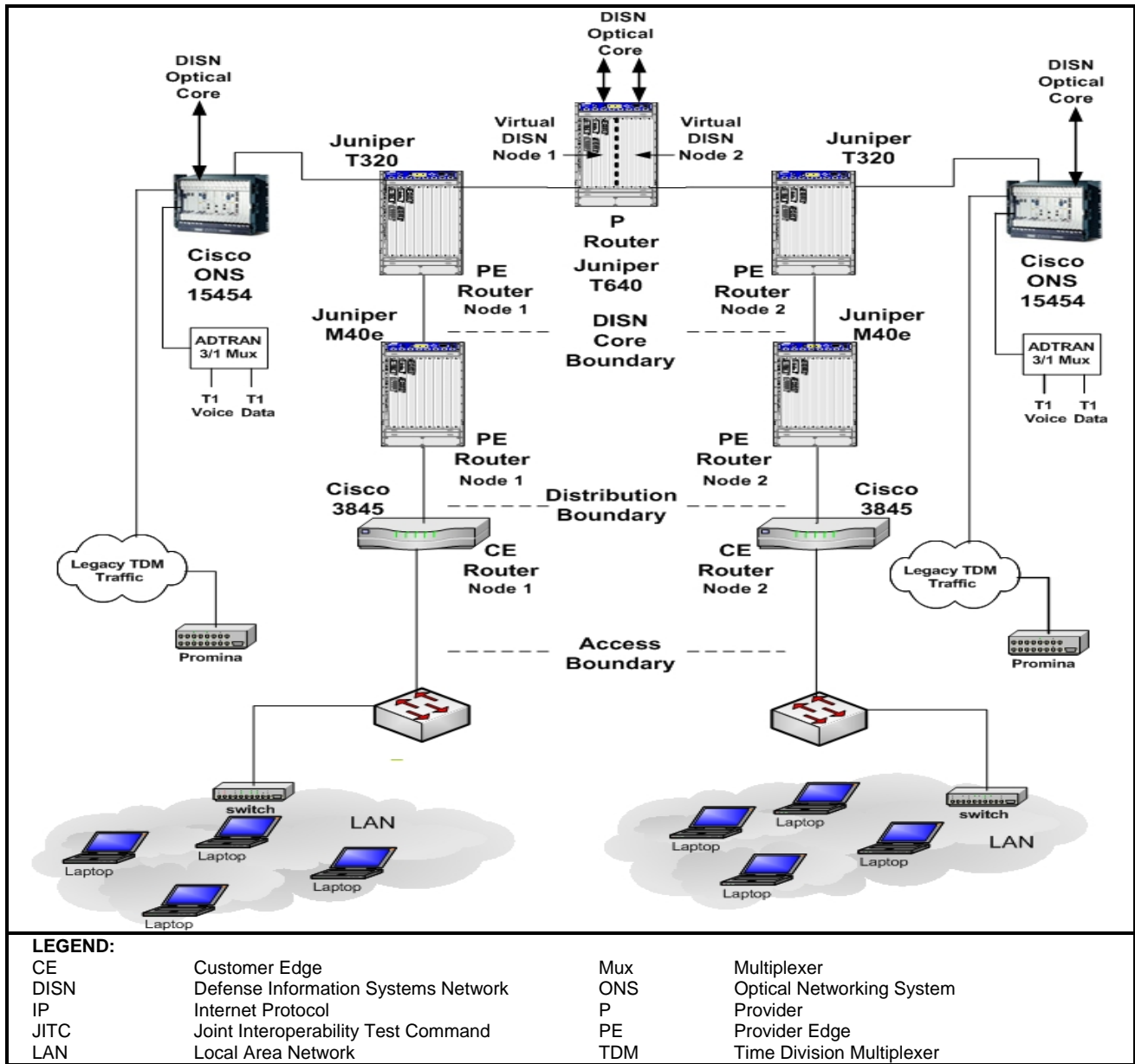


Figure 2-1. JITC Simulated DISN IP Core Node

7. REQUIRED DEVICE INTERFACES. All IPv6-capable products to be included on the DoD IPv6 Approved Product List must meet the requirements of the DoD Information Technology Standards Registry (DISR) DoD IPv6 Standard Profiles for IPv6 Capable Products Version 1, 1 June 2006. Product testing against these requirements is conducted in accordance with the DoD IPv6 Generic Test Plan (GTP) Version 3, Draft. The DoD IPv6 GTP Version 3 includes more accurate test procedures and a complete IPSec annex and therefore was used for this test instead of the DoD IPv6 GTP Version 2. The IPv6 router profile requirements are conformance, performance, and interoperability and are listed in table 2-1.

Table 2-1. IPv6 Capability Requirements and Status

Cisco 1800, 2800, 3800, and 7200 Family of Routers								
RFC	RFC Title	Testing Completed			Router		Implemented	Comments
		Conformance	Performance	Interoperability	Requirement	Met/Not Met		
IPv6 Base								
1981	Path Maximum Transmission Unit Discovery for IPv6	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2460	Internet Protocol version 6 (IPv6) Specification	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2461	Neighbor Discovery for IP version 6 (IPv6)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2462	IPv6 Stateless Address Auto configuration	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2464	Transmission of IPv6 Packets over Ethernet Networks	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2710	Multicast Listener Discovery (MLD)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4007	IPv6 Scoped Address Architecture	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4193	Unique Local IPv6 Unicast Addresses	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4291	IPv6 Addressing Architecture	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
IPSec								
2401	Security Architecture for IP	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2402	IP Authentication Header (AH)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2406	IP Encapsulating Security Payload	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2407	The Internet Security Domain of Interpretation for ISAKMP	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 1800, 2800, 3800, and 7200 Family of Routers								
RFC	RFC Title	Testing Completed			Router		Implemented	Comments
		Conformance	Performance	Interoperability	Requirement	Met/Not Met		
2408	Internet Security Association and Key Management Protocol	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2409	Internet Key Exchange (IKE)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4301	Security Architecture for Internet Protocol	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4302	IP Authentication Header	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4303	IP Encapsulating Security Payload (ESP)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4306	Internet Key Exchange (IKEv2) Protocol	Not Listed	Not Tested	Not Tested	O	Not Tested	No	See Note
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	Not Listed	Not Tested	Not Tested	O	Not Tested	No	See Note
4308	Cryptographic Suites for IPsec	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Transition Mechanisms								
2784	Generic Routing Encapsulation (GRE)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
4213	Transition Mechanisms for IPv6 Host and Routers	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Quality of Service								
2474	Definition of the DiffServ Field in the IPv4 and IPv6 Headers	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 1800, 2800, 3800, and 7200 Family of Routers								
RFC	RFC Title	Testing Completed			Router		Implemented	Comments
		Conformance	Performance	Interoperability	Requirement	Met/Not Met		
Mobility								
3775	Mobility Support in IPv6	Not Listed	Not Tested	Not Tested	O	Not Tested	No	See Note
3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	Not Listed	Not Tested	Not Tested	O	Not Tested	No	See Note
3963	Network Mobility (NEMO) Basic Support Protocol	Not Listed	Not Tested	Not Tested	O	Not Tested	No	See Note
Network Management								
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
3413	Simple Network Management Protocol (SNMP) Applications	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Interior Router								
2473	Generic Packet Tunneling in IPv6 Specification	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2740	OSPF for IPv6	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
Exterior Router								
1772	Application of the Border Gateway Protocol in the Internet	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2545	Border Gateway Protocol Extensions for IPv6 Interdomain Routing	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	
2858	Multiprotocol Extensions for BGP-4	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes	

Table 2-1. IPv6 Capability Requirements and Status (continued)

Cisco 1800, 2800, 3800, and 7200 Family of Routers																																				
RFC	RFC Title	Testing Completed			Router		Implemented	Comments																												
		Conformance	Performance	Interoperability	Requirement	Met/Not Met																														
4271	A Border Gateway Protocol 4 (BGP-4)	Stated in LoC	No Performance Test Required	Yes	R	Met	Yes																													
<p>LEGEND:</p> <table border="0"> <tr> <td>BGP-4</td> <td>Border Gateway Protocol Version 4</td> <td>LoC</td> <td>Letter of Conformance</td> </tr> <tr> <td>DiffServ</td> <td>Differentiated Services</td> <td>N/R</td> <td>Not Required</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>O</td> <td>Optional</td> </tr> <tr> <td>IPSec</td> <td>Internet Protocol Security</td> <td>OSPF</td> <td>Opened Shortest Path First</td> </tr> <tr> <td>IPv4</td> <td>Internet Protocol Version 4</td> <td>R</td> <td>Required</td> </tr> <tr> <td>IPv6</td> <td>Internet Protocol Version 6</td> <td>RFC</td> <td>Request for Comments</td> </tr> <tr> <td>ISAKMP</td> <td>Internet Security Association and Key Management Protocol</td> <td></td> <td></td> </tr> </table> <p>NOTE: Conformance, Performance, and Interoperability testing was not completed for the RFC due to the devices' requirements being "Optional," therefore; it was "Not Tested." In cases where "Optional" RFCs were tested, the vendor requested the test.</p>									BGP-4	Border Gateway Protocol Version 4	LoC	Letter of Conformance	DiffServ	Differentiated Services	N/R	Not Required	IP	Internet Protocol	O	Optional	IPSec	Internet Protocol Security	OSPF	Opened Shortest Path First	IPv4	Internet Protocol Version 4	R	Required	IPv6	Internet Protocol Version 6	RFC	Request for Comments	ISAKMP	Internet Security Association and Key Management Protocol		
BGP-4	Border Gateway Protocol Version 4	LoC	Letter of Conformance																																	
DiffServ	Differentiated Services	N/R	Not Required																																	
IP	Internet Protocol	O	Optional																																	
IPSec	Internet Protocol Security	OSPF	Opened Shortest Path First																																	
IPv4	Internet Protocol Version 4	R	Required																																	
IPv6	Internet Protocol Version 6	RFC	Request for Comments																																	
ISAKMP	Internet Security Association and Key Management Protocol																																			

8. TEST NETWORK DESCRIPTION. The routers were tested as part of a simulated DISN IP Core Node test architecture managed by the Advanced IP Technology Laboratory at JITC, and configured as shown in figure 2-2.

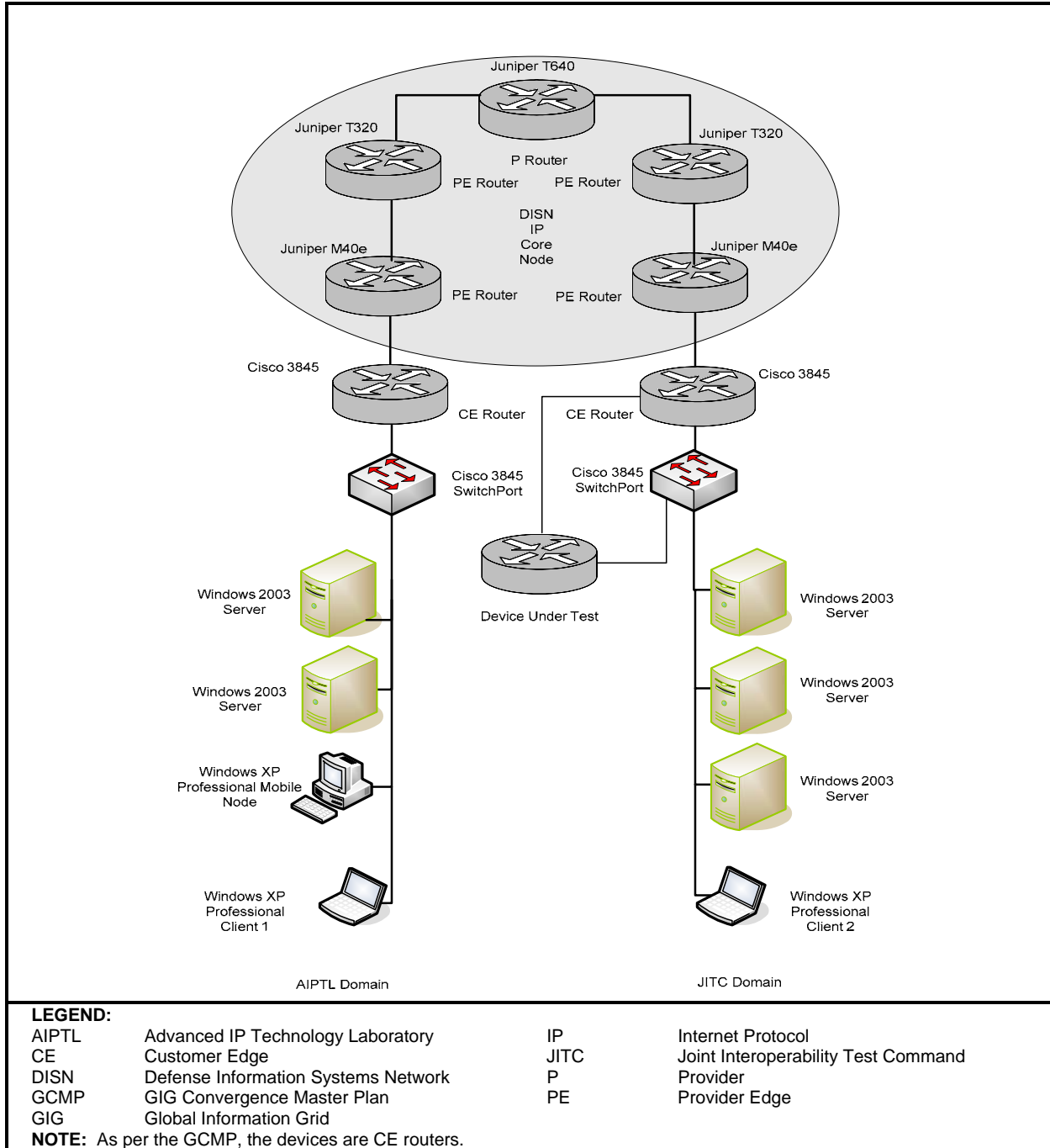


Figure 2-2. JITC Simulated DISN IP Core Node Test Network

The core consisted of one Juniper T640, two Juniper T320 routers, two Juniper M40e routers, two Cisco 3845 routers, five Dell Power Edge 2850 Servers, one Gateway personal computer (PC) and two Gateway notebooks. All PCs were loaded with MS Windows XP Professional and an IP Packet capturing tool, Wireshark. Client 2 was loaded with SimpleTesterPro for Simple Network Management Protocol (SNMP) testing.

9. DEVICE CONFIGURATIONS. Table 2-2 provides hardware and software components used in the test network.

Table 2-2. Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS/Version(s)
Hardware		
Cisco Router - DUT	Cisco 1841	12.4(11)T
Cisco Router - DUT	Cisco 2811	12.4(11)T
2 Cisco Routers - 1 DUT	Cisco 3845	12.4(11)T
Cisco Router - DUT	Cisco 7200	12.4(11)T
2 Juniper Routers	Juniper M40e	V 7.4R2.6/V 7.6R3.6
2 Juniper Routers	Juniper T320	V 7.4R2.6
Juniper Router	Juniper T640	V 7.1R3.3/V 7.4R2.6
5 Dell Power Edge Servers	2850	MS 2003 Server
2 Gateway Notebooks	450ROG	Windows XP Professional
Gateway Workstation	E Series	Windows XP Professional
Software		
Windows XP Professional	N/A	Build 5.1.2600 SP2
Windows Server 2003	N/A	Build 5.2.3790 SP1
SimpleTesterPro	N/A	V11.0.1
VLC Media Player	N/A	V0.8.6b
Wireshark	N/A	V.0.99.2
LEGEND:		
DUT	Device Under Test	R Release
IOS	Internetwork Operating System	SP Service Pack
MS	Microsoft	T New Technology
N/A	Not Applicable	V Version
OS	Operating System	VLC VideoLAN Client

10. TEST LIMITATIONS. None.

11. TEST RESULTS.

a. IPv6 Base.

Test Case C.1.1. The RFC 1981 Path Maximum Transmission Unit Discovery for IPv6 is necessary for proper IPv6 implementations. It acts as a mechanism to determine the maximum size of packets to traverse the network without fragmentation. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.2. The RFC 2460 IPv6 Specification is the base specification of the IPv6 protocol. It specifies a number of parameters that enable successful completion of IPv6 traffic addressing and control. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.3. The RFC 2461 Neighbor Discovery for IPv6 specifies the neighbor discovery function that is similar to address resolution protocol in IP Version 4 (IPv4). It is necessary for implementing neighbor solicitations and neighbor advertisements within IPv6. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.4. The RFC 2462 IPv6 Stateless Address Auto-configuration specifies how a host auto-configures its interfaces in IPv6. These steps include determining whether the source addressing should be stateless or stateful, whether the information obtained should be solely the address or include other information, and Duplicate Address Detection. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.5. The RFC 2464 Transmission of IPv6 Packets over Ethernet Networks specifies the frame format for transmission of IPv6 link-local addresses and statelessly auto-configured addresses on Ethernet networks. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.8. The RFC 2710 Multicast Listener Discovery (MLD) for IPv6 specifies the protocol used by an IPv6 router to discover the presence of multicast listeners (i.e., nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.10. The RFC 3810 MLD Version 2 (MLDv2) is used by IPv6 routers to discover the presence of multicast listeners on their directly attached links, and to discover specifically which multicast addresses are interests to those neighboring node. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.11. The RFC 4007 IPv6 Scoped Address Architecture defines the nature and characteristics for the usage of IPv6 addresses of different scopes. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.1.12. The RFC 4193 Unique Local IPv6 Unicast Addresses defines the address format and how it is globally unique. Local IPv6 unicast addressing is intended to be used for local communications and is not expected to be routed to the Internet. Cisco routers 1841, 2811, 3845 and 7200 met the test requirements.

Test Case C.1.13. The RFC 4291 IPv6 Addressing Architecture defines the

specifications for the addressing architecture of the IPv6 protocol. The definitions cover unicast addresses, anycast addresses, and multicast addresses. Cisco routers 1841, 2811, 3845 and 7200 met the test requirements.

Test Case C.1.14. The RFC 4443 identifies Internet Control Message Protocol messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

b. IPSec.

Test Case C.2.1. The RFC 2401 Security Architecture for the IP specifies the base architecture for IPSec compliant systems. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.2. The RFC 2402 IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams to provide protection against replays. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.3. The RFC 2406 IP Encapsulating Security Payload (ESP) headers are designed to provide a mix of security services in IPv4 and IPv6. The ESP may be applied alone, in combination with the IP AH, or in a nested fashion (e.g., through the use of tunnel mode). Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.4. The RFC 2407 Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.4. The RFC 2408 ISAKMP describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.4. The RFC 2409 Internet Key Exchange (IKE) describes a protocol using part of Oakley and part of Secure Key Exchange Mechanism (SKEME) in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other SAs such as AH and ESP for Internet Engineering Task Force IPSec Domain of Interpretation. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.1. The RFC 4301 Security Architecture for the IP specifies the base

architecture for IPSec-compliant systems. It describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.2. The RFC 4302 IP AH is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.3. The RFC 4303 IP ESP is designed to provide a mix of security services in IPv4 and IPv6. The ESP may be applied alone, in combination with AH, or in a nested fashion. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.4. The RFC 4305 Cryptographic Algorithm Implementation Requirements for ESP and AH defines the ability to successfully establish IPSec utilizing all of the required encryption and authentication algorithms. The DUT will be able to communicate over the established IPSec links using IPv6. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.2.7. The RFC 4308 Cryptographic Suites for IPSec suites should not be considered extensions to IPSec, IKE, and IKEv2, but instead administrative methods for describing sets of configurations. The IPSec, IKE, and IKEv2 protocols rely on security algorithms to provide privacy and authentication between the initiator and responder. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

c. Transition Mechanisms.

Test Case C.3.6. The RFC 2784 Generic Routing Encapsulation is a protocol for encapsulation of an arbitrary Network Layer Protocol (NLP) over another arbitrary NLP when a system has a payload packet that needs to be encapsulated and delivered to some destination. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.19. The RFC 4213 Transition Mechanisms for IPv6 Host and Routers specifies IPv4 co-existence mechanisms that can be implemented by IPv6 devices. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

d. Quality of Service.

Test Case C.3.3. The RFC 2474 Definition of the Differentiated Services (DiffServ) Field in the IPv4 and IPv6 Headers defines the DiffServ field. In IPv4, it defines the layout of the Type-of-Service octet and in IPv6, the Traffic Class octet. In addition, a base set of packet forwarding treatments, or per-hop behaviors, is defined. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

e. Network Management.

Test Case C.3.10. The RFC 3411 An Architecture for Describing SNMP Management Frameworks is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major portions of the architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem, and an Access Control Subsystem, and possibly multiple SNMP applications, which provide specific functional processing of management data. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.11. The RFC 3412 Message Processing and Dispatching for the SNMP describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching Protocol Data Units to SNMP applications. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.12. The RFC 3413 SNMP Applications describes five types of SNMP applications which make use of an SNMP engine as described in Standard 62, RFC 3411. The types of application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

f. Interior Router.

Test Case C.3.2. The RFC 2473 Generic Packet Tunneling in IPv6 Specification defines the model and generic mechanisms for IPv6 encapsulation of IPv6 and IPv4 packets. The model and mechanisms can be applied to other protocol packets such as AppleTalk, Internetwork Packet Exchange (IPX), Connectionless Network Protocol, and/or others. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.5. The RFC 2740 Open Shortest Path First (OSPF) for IPv6 handles the increased address size of IPv6. The fundamental mechanisms of OSPF (flooding, Designated Router election, OSPF area support, Shortest Path First algorithms) remain unchanged. However, addressing semantics have been removed from OSPF packets and the basic Link State Advertisements (LSA). New LSA have been created to carry IPv6 addresses and prefixes. The OSPF now runs on a per-link basis, instead of on a per-IP-subnet basis. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

g. Exterior Router.

Test Case C.3.1. The RFC 1772 Application of the Border Gateway Protocol (BGP) in the Internet is an inter-Autonomous System routing protocol. Based on performance, preference, and policy constraints, the network reachability information exchanged via

BGP provides sufficient information to detect routing loops and enforce routing decisions. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.4. The RFC 2545 BGP Extensions for IPv6 Interdomain Routing describes two BGP attributes (MP_REACH_NLRI and MP_UNREACH_NLRI) that can be used to announce and withdraw the announcement of reach ability information. The RFC defines how systems should make use of these attributes for conveying IPv6 routing information. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.20. The RFC 2858 Multiprotocol Extensions for BGP Version 4 (BGP-4) allows the use of extensions to enable BGP-4 to carry routing information for multiple NLP (e.g., IPv6 or IPX). A router that supports the extensions can interoperate with a router that does not support the extensions thus making the extensions backward compatible. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

Test Case C.3.20. The RFC 4271 BGP-4 is capable of carrying routing information only for IPv4. This RFC defines extensions to BGP-4 to enable it to carry routing information for multiple NLPs (e.g., IPv6 or IPX). The extensions are backward compatible - a router that supports the extensions can interoperate with a router that does not support the extensions. Cisco routers 1841, 2811, 3845, and 7200 met the test requirements.

h. Conclusion. Cisco routers 1841, 2811, 3845, and 7200 routers met all the required RFCs.

12 TEST AND ANALYSIS REPORT. No detailed test report was written in accordance with the DoD IPv6 Master Test Plan. All test data is maintained in the Advanced IP Technology Laboratory and is available upon request. This certification is available on the Joint Interoperability Tool (JIT). The JIT homepage is <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125/> (SIPRNet). The JIT has links to JITC interoperability documents to provide the DoD community, including the warfighter in the field, easy access to the latest interoperability information. System interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at: <https://stp.fhu.disa.mil/>.